

NON-VANISHING OF DIRICHLET L -FUNCTIONS IN GALOIS ORBITS

RIZWANUR KHAN, DJORDJE MILIĆEVIĆ, AND HIEU T. NGO

ABSTRACT. A well known result of Iwaniec and Sarnak states that for at least one third of the primitive Dirichlet characters to a large modulus q , the associated L -functions do not vanish at the central point. When q is a large power of a fixed prime, we prove the same proportion already among the primitive characters of any given order. The set of primitive characters modulo q of a given order can be described as an orbit under the action of the Galois group of the corresponding cyclotomic field. We also prove a positive proportion of nonvanishing within substantially shorter orbits generated by intermediate Galois groups as soon as they are larger than roughly the square-root of the prime-power conductor.

1. INTRODUCTION

Central values of L -functions are of fundamental importance in number theory. In particular, a host of results and conjectures, including the Birch and Swinnerton-Dyer Conjecture, the Riemann Hypothesis, and the Katz-Sarnak Density Conjecture, predict in various contexts that the central values of L -functions (or their derivatives, as appropriate for root number reasons) hold key arithmetic information and should vanish only when there are deep arithmetic reasons for them to do so and that this should be an exceptional occurrence in suitably generic families.

Introduced by Bohr and Landau [3] in their study of zeroes of the Riemann zeta-function and notably used by Selberg [17] in the course of proving that a positive proportion of these zeroes lie on the critical line, the “mollifier” is the most versatile tool used in analytic number theory to prove the non-vanishing of central values of L -functions in families, often achieving a positive proportion result. What is by now a classical result using the mollifier is one of Iwaniec and Sarnak [10], concerning non-vanishing in the family of Dirichlet L -functions. They proved that for at least $(\frac{1}{3} - \epsilon)$ of the primitive Dirichlet characters modulo q , where q is any integer sufficiently large in terms of ϵ , the central value $L(\frac{1}{2}, \chi)$ is not zero. This is currently the best known result that can be proved with a “one-piece” mollifier. Earlier, Balasubramanian and Murty [1] had established a smaller positive proportion of non-vanishing, and recently, Bui [5] proved, using a “two-piece” mollifier, that about 34% of the central values in this family do not vanish. When one restricts to the quadratic Dirichlet L -functions, Soundararajan [21] established that for at least $\frac{7}{8}$ of the fundamental discriminants $|d| \leq X$, the central value $L(\frac{1}{2}, (\frac{d}{\cdot}))$ is not zero, as $X \rightarrow \infty$. It is generally conjectured (see the discussion in [21]) that

$$(1.1) \quad L(\tfrac{1}{2}, \chi) \neq 0$$

2010 *Mathematics Subject Classification.* Primary: 11M20, Secondary: 11J61.

Key words and phrases. L -functions, Dirichlet characters, non-vanishing, mollifier, depth aspect, p -adic Roth’s theorem.

D.M. acknowledges support by the National Security Agency. Project is sponsored by the NSA under Grant Number H98230-14-1-0139. The United States Government is authorized to reproduce and distribute reprints notwithstanding any copyright notation herein.

for any primitive character χ . Such a statement appears to be substantially beyond the reach of currently available technology.

Let ξ be a primitive $\phi(q)$ -th root of unity, where ϕ is the Euler totient function. The Galois group $G = \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ acts on the set of primitive Dirichlet characters modulo q as follows. For $\sigma \in G$, we define χ^σ to be the character given by $\chi^\sigma(n) = \sigma(\chi(n))$ for all integers n . The Galois action partitions the set of characters into orbits, which are particularly natural from the arithmetic point of view, since the associated Dirichlet L -functions (by definition) share the same field of coefficients. One is led to wonder whether a positive proportion of non-vanishing can be proven for Dirichlet L -functions within each orbit. The aforementioned results [10] and [5] do not preclude the possibility that $L(\frac{1}{2}, \chi) = 0$ for all χ in some orbit \mathcal{O} .

As a positive proportion statement toward (1.1) in this context, we conjecture that for some $c > 0$, we have that

$$(1.2) \quad \frac{1}{|\mathcal{O}|} \sum_{\substack{\chi \in \mathcal{O} \\ L(\frac{1}{2}, \chi) \neq 0}} 1 \geq c - \epsilon$$

for any $\epsilon > 0$, any orbit \mathcal{O} of cardinality $|\mathcal{O}| > q^\epsilon$, and any integer q sufficiently large in terms of ϵ . One might hope to match the best constant $c = 0.34$ currently available for the full set of primitive Dirichlet L -functions or the more classical proportion of Iwaniec and Sarnak. We establish the latter in the case that q is a large power of a prime.

Theorem 1.1. *Let $q = p^k$ for an odd prime p . For any $\epsilon > 0$ and k large enough in terms of ϵ and p , we have that (1.2) holds with $c = \frac{1}{3}$.*

When $q = p^k$, the orbits under the Galois action can be described as follows. First recall that a necessary and sufficient condition for the existence of a *primitive* character modulo p^k having order l is that $l = p^{k-1}d$ for some $d \mid (p-1)$. The set of all primitive Dirichlet characters modulo q whose orders equal $p^{k-1}d$ forms an orbit \mathcal{O} of cardinality

$$(1.3) \quad |\mathcal{O}| = \phi(p^{k-1}d),$$

and every orbit arises in this way. Thus \mathcal{O} depends on d but we suppress this in the notation. For these facts, see, for example, [7, Chapter 5] and [6, page 16].

Although, from an analytic perspective, it may appear that we are dealing with a family only slightly thinner than the original unitary family of all primitive Dirichlet characters, in reality this gives rise to a significant difficulty, which we describe below in the introduction. The key feature here is that the family is “thinning out” in a thoroughly arithmetic (rather than analytic) way. In fact, the same device that we use to overcome this basic difficulty subsequently allows us to prove a positive proportion of non-vanishing in substantially smaller “thin orbits” in Theorem 1.3 below.

The problem of studying the non-vanishing of L -functions within Galois orbits is a natural one that has yielded some of the strongest known results in the subject. Let $q = p^k$ for the remainder of this paper. Let f be a holomorphic newform of weight 2 and level coprime to p which has rational Fourier coefficients (equivalently, f is associated to an elliptic curve over \mathbb{Q} of conductor coprime to p , by [20, Theorems 7.14, 7.15] and [23, 22, 4]). Let $L(s, f \times \chi)$ be the L -function of f twisted by a primitive Dirichlet character χ modulo q , having central point $s = 1$ by a functional equation normalized so as to relate $L(s, f \times \chi)$ and $L(2-s, f \times \overline{\chi})$. Rohrlich [16] showed that $L(1, f \times \chi)$ does not vanish as long as k is large enough in terms of p and f . To prove his result, Rohrlich appealed

to an “algebraicity” theorem of Shimura [18, 19, Theorem 1], which implies that if $L(1, f \times \chi) = 0$ then $L(1, f \times \chi^\sigma) = 0$ for all $\sigma \in G$. By this, if the sum

$$(1.4) \quad \sum_{\chi \in \mathcal{O}} L(1, f \times \chi)$$

is nonzero, then every summand is nonzero. Rohrlich found an asymptotic for (1.4) for any orbit \mathcal{O} when k is large enough in terms of p and f , and showed that the main term is indeed nonzero. Chinta [6] extended Rohrlich’s work to the case of prime moduli q by considering instead the sum

$$(1.5) \quad \sum_{\chi \in \mathcal{O}} L(1, f \times \chi) M(f \times \chi),$$

where $M(f \times \chi)$ is a truncation of the formal Dirichlet series for $L(1, f \times \chi)^{-1}$. The effect of this mollifier is that each summand of (1.5) is “morally” close to 1, and this allows Chinta to show that the sum is nonzero provided $|\mathcal{O}| > q^{\frac{1}{2}+\epsilon}$ and q is large enough in terms of f . In particular, this implies the non-vanishing of $L(1, f \times \chi)$ over big orbits when q is a large enough prime in terms of f , a fact which does not follow from Rohrlich’s result.

All these results for twists of elliptic modular L -functions rely heavily on the algebraicity results of Shimura. Such a route is not available in the present context of central values of Dirichlet L -functions.

We establish Theorem 1.1 by evaluating the mollified moments

$$(1.6) \quad \sum_{\chi \in \mathcal{O}} L(\tfrac{1}{2}, \chi) M(\chi)$$

and

$$(1.7) \quad \sum_{\chi \in \mathcal{O}} |L(\tfrac{1}{2}, \chi)|^2 |M(\chi)|^2,$$

where

$$(1.8) \quad M(\chi) = \sum_{m \leq q^\theta} \frac{a_m \chi(m)}{m^{\frac{1}{2}}}$$

is a mollifier of length q^θ , for some $\theta \geq 0$ and coefficients a_m satisfying $a_m \ll m^\epsilon$ and $a_1 = 1$. We are able to obtain asymptotics with a power-saving error term for arbitrary mollifiers when θ is any fixed constant satisfying $0 \leq \theta < \frac{1}{2}$; see Propositions 2.4 and 2.5. As discussed in section 2.3, this allows us to deduce Theorem 1.1 with the proportion of non-vanishing $c = \frac{1}{3}$ by taking $\theta \rightarrow \frac{1}{2}$.

Although $|L(\frac{1}{2}, \chi)|^2$ can be considered to be analogous to $L(1, f \times \chi)$, our problem has some important differences from the one considered by Rohrlich and Chinta. Firstly, the additional factor $|M(\chi)|^2$ in (1.7) makes our problem more complex. This is readily seen when comparing with (1.4), and to compare with (1.5) we note that Chinta’s method only works for a specific mollifier while ours works for an arbitrary mollifier, and that $M(f \times \chi)$ has length at most $q^{\frac{1}{4}-\epsilon}$ (see [6, pg 22]) while $|M(\chi)|^2$ has length at most $q^{1-\epsilon}$. However one must keep in mind that Chinta proves a result which works for q prime, while ours does not.

The second difference is the method of proof. To evaluate (1.4), Rohrlich had to consider the averages

$$(1.9) \quad \sum_{\chi \in \mathcal{O}} \chi(n)$$

for $n \leq q^{1+\epsilon}$, while for (1.7) we must consider the averages

$$(1.10) \quad \sum_{\chi \in \mathcal{O}} \chi(n_1 m_1) \overline{\chi}(n_2 m_2)$$

in which $n_1 n_2 \leq q^{1+\epsilon}$ and $m_1, m_2 \leq q^\theta$. As we will see, (1.9) is zero unless $n^{p-1} \equiv 1 \pmod{p^{k-1}}$. From this, Rohrlich could immediately conclude that $n = 1$ or $n > p^{\frac{k-1}{p-1}}$, thereby effectively isolating the contribution of the diagonal term $n = 1$. In contrast, (1.10) is zero unless

$$(1.11) \quad (n_1 m_1)^{p-1} \equiv (n_2 m_2)^{p-1} \pmod{p^{k-1}}.$$

Writing $n_1 m_1 \equiv \zeta n_2 m_2 \pmod{p^k}$, it is now much harder to isolate the contribution of the diagonal terms $n_1 m_1 = n_2 m_2$ (that is, $\zeta \equiv 1 \pmod{p^k}$); *a priori* it is, for example, perfectly plausible that $n_1 m_1$ and $n_2 m_2$ could be fairly close to each other without actually being equal. To isolate the contribution of the diagonal terms $n_1 m_1 = n_2 m_2$, we will appeal to the p -adic version of Roth's theorem, Lemma 2.6 below. The upshot is that, keeping in mind that $\zeta^{p-1} \equiv 1 \pmod{p^k}$, having two solutions to (1.11) within the same class of $\zeta \not\equiv \pm 1 \pmod{p^k}$ too close to each other would ultimately yield too good of an approximation in the p -adic norm to a $(p-1)^{\text{th}}$ p -adic root of unity.

It is interesting that Roth's theorem, a deep result from diophantine approximation, should be used to prove the non-vanishing of L -functions. This connection has been made before in different contexts by Rohrlich [15] and Greenberg [8]. Our paper offers another such example and it seems to be the first one involving a family of Dirichlet characters as well as the first one involving a genuinely second mollified moment.

Taking $\theta = 0$ in our evaluation of (1.6) and (1.7) yields in particular the first and second moments of $L(\frac{1}{2}, \chi)$ over Galois orbits. Before stating this result, we note that the value $\chi(-1)$ is the same for every character in any given orbit \mathcal{O} , as it is a rational number.

Theorem 1.2. *Let $q = p^k$ for an odd prime p and let \mathcal{O} be any Galois orbit of primitive Dirichlet characters mod q . Suppose that $\chi(-1) = (-1)^\iota$ for any $\chi \in \mathcal{O}$. We have that*

$$\begin{aligned} \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} L(\tfrac{1}{2}, \chi) &= 1 + O(q^{-\frac{1}{4}+\epsilon}) \\ \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} |L(\tfrac{1}{2}, \chi)|^2 &= \frac{p-1}{p} \left(\log\left(\frac{q}{\pi}\right) + \frac{\Gamma'(\frac{1+2\iota}{4})}{\Gamma(\frac{1+2\iota}{4})} + 2\gamma + 2\frac{\log p}{p-1} \right) + O(q^{-\frac{1}{4}+\epsilon}), \end{aligned}$$

for any $\epsilon > 0$, where the implied constants depend on ϵ and p , and $\gamma = 0.57721 \dots$ is the Euler constant.

We remark that the implicit constants in all our main results are ineffective due to their dependence on p -adic Roth's Theorem. However, the first moment in Theorem 1.2 and the mollified first moment in Proposition 2.4 can also be evaluated without recourse to p -adic Roth's Theorem, at the expense of the error terms $O(q^{-\frac{1}{4}+\epsilon})$ being replaced by the weaker but effective error terms $O(q^{-\frac{1}{2(p-1)}+\epsilon})$. This will be shown in the course of the proof of Proposition 2.4.

Finally, we address the refined question of non-vanishing in smaller sub-families within the Galois orbits of primitive characters modulo q . A rather natural sub-family emerges when considering orbits of primitive characters under various subgroups H of the Galois group $G = \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$. These subgroups form a partially ordered set (corresponding by Galois theory to the tree of intermediary field extensions $\mathbb{Q} \leq K \leq \mathbb{Q}(\xi)$), and, as the subgroup H varies from G through its various

subgroups to the identity, the corresponding orbits of a fixed primitive character modulo q can be seen as interpolating (or shrinking) between its full Galois orbit, considered in Theorem 1.1, and the individual character.

We describe these “thin orbits” explicitly in cases of our interest. For every $0 \leq \kappa \leq k-1$, denote $K_{k-1-\kappa} = \mathbb{Q}(\xi^{p^\kappa})$. (Note that the field K_ℓ is independent of k .) Since $[K_{k-1} : K_0] = \phi(p^{k-1}) \asymp_p \phi(\phi(q))$ and we are primarily concerned with the case of fixed p and large k , we focus here on the tower of these intermediate fields

$$\mathbb{Q}(\xi) = K_{k-1} \supseteq \cdots \supseteq K_0 \supseteq \mathbb{Q}.$$

The Galois group $\text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ acts transitively on any given Galois orbit \mathcal{O} . The intermediate Galois group $\text{Gal}(\mathbb{Q}(\xi)/K_{k-1-\kappa})$ therefore acts on \mathcal{O} ; we call an orbit of this action a *thin Galois orbit*, and we write \mathcal{O}_κ for any one of these thin orbits. Note that already the thin orbits \mathcal{O}_{k-1} refine the full Galois orbits \mathcal{O} , with thin orbits \mathcal{O}_κ for smaller κ being progressively smaller (so that we may think of the parameter κ essentially as an indicator or the logarithmic size of the corresponding thin orbits), all the way to the extreme case of $\kappa = 0$, which corresponds to the single primitive characters.

It is not difficult to see that $\sigma \in \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ satisfies $\sigma \in \text{Gal}(\mathbb{Q}(\xi)/K_{k-1-\kappa})$ if and only if

$$(1.12) \quad \sigma(\xi) = \xi^a \quad \text{for some } a \equiv 1 \pmod{p^{k-1-\kappa}(p-1)}.$$

We thus see that, equivalently, two characters χ_1, χ_2 are in the same thin Galois orbit \mathcal{O}_κ if and only if $\chi_1 \overline{\chi_2}$ has order dividing p^κ (informally speaking, if χ_1 and χ_2 differ by an “algebraically simpler” character, one that is “shallower” in the sense of the “depth aspect” of modulus $q = p^k$ with large k). In particular, all thin orbits \mathcal{O}_κ for the same κ are of equal size given by (keeping in mind that $(a, \phi(q)) = 1$)

$$|\mathcal{O}_\kappa| = \begin{cases} p^\kappa, & 0 \leq \kappa < k-1, \\ \phi(p^{k-1}), & \kappa = k-1. \end{cases}$$

Another, more “analytic”, way to think about the thin orbits \mathcal{O}_κ is provided by the explicit characterization of the “principal part” of the dual of the group $(\mathbb{Z}/q\mathbb{Z})^\times$ for a high prime power $q = p^k$, which is essentially due to Postnikov [13]. Let $X_k = (\mathbb{Z}/p^k\mathbb{Z})^\times$, and let π_a denote the power map $\pi_a : X_k \rightarrow X_k$, $[x] \mapsto [x^a]$. Corresponding to the decomposition $X_k = X_{k0} \times X_{k1}$, where $X_{k0} = \text{im } \pi_{p^{k-1}} = \ker \pi_{p-1}$, $|X_{k0}| = p-1$, and $X_{k1} = \text{im } \pi_{p-1} = \ker \pi_{p^{k-1}} = \{[x] \in X_k : x \equiv 1 \pmod{p}\}$, we have the canonical decomposition of dual groups $\hat{X}_k \cong \hat{X}_{k0} \times \hat{X}_{k1}$. Let \log_p denote the p -adic logarithm and $\psi(x)$ denote the “standard” additive character $\psi : \mathbb{Q}_p \rightarrow \mathbb{C}^\times$ such that its kernel is exactly \mathbb{Z}_p and that $\psi(x) = e^{2\pi i x}$ for $x \in \mathbb{Z}[1/p] \subseteq \mathbb{Q}_p \cap \mathbb{R}$. According to Postnikov’s lemma (for $p > 2$; see also [12, Lemma 13]), every character $\chi^{(1)} \in \hat{X}_{k1}$ is of the form

$$\chi^{(1)}(1+pt) = \chi_a^{(1)}(1+pt) = \psi\left(\frac{a_0 \log_p(1+pt)}{p^k}\right)$$

for some $a = a_0 p^{-k} \in p^{-k}\mathbb{Z}_p/p^{-1}\mathbb{Z}_p$, with primitive characters corresponding to $a \in p^{-k}\mathbb{Z}_p^\times/p^{-1}\mathbb{Z}_p$.

The isomorphism of $p^{-k}\mathbb{Z}_p/p^{-1}\mathbb{Z}_p \rightarrow \hat{X}_{k1}$ given by $a \mapsto \chi_a^{(1)}$ induces a metric on \hat{X}_{k1} via $d(\chi_a^{(1)}, \chi_b^{(1)}) = |a-b|_p/p = \text{cond}(\bar{\chi}_a^{(1)} \chi_b^{(1)})$ for $\chi_a^{(1)} \neq \chi_b^{(1)}$. Relative to the above decomposition of \hat{X}_k and this metric on \hat{X}_{k1} , the thin orbit \mathcal{O}_κ containing a character $\chi = \chi^{(0)} \chi^{(1)}$ is, for $\kappa > 0$, precisely the set $\{\chi^{(0)}\} \times B[\chi^{(1)}, p^\kappa]$; here $B[\chi^{(1)}, p^\kappa]$ denotes the closed ball in \hat{X}_{k1} with center $\chi^{(1)}$ and radius p^κ with respect to the above-defined metric. In particular, all characters in a thin orbit

\mathcal{O}_κ share the same \hat{X}_{k0} -component and their \hat{X}_{k1} -components are all close to each other, with the corresponding neighborhood around a fixed character χ shrinking as κ decreases.

From the point of view of harmonic analysis, we see clearly the basic difficulty of isolating individual $\chi^{(0)} \in \hat{X}_{k0}$ in our orbits (which, in a modified form, is already present in isolating the full orbits \mathcal{O}), which on the dual side is reflected by the initial survival of the $(p-1)^{\text{th}}$ roots of unity in Lemma 3.1, followed by isolating characters $\chi^{(1)}$ in smaller neighborhoods within \hat{X}_{k1} , which corresponds to the survival of further terms in more permissive congruence classes containing these roots of unity.

Our techniques, which ultimately rely on the impossibility of overly good p -adic approximations to algebraic integers, are very well suited to the study of thin orbits of primitive characters to prime power moduli and give the following refinement of Theorem 1.1.

Theorem 1.3. *Let $q = p^k$ for an odd prime p . For any $\epsilon > 0$ and k large enough in terms of ϵ and p , and for any $\kappa > k/2$, we have that (1.2) holds also when \mathcal{O} is replaced by any “thin orbit” \mathcal{O}_κ , with*

$$c = c_\kappa = \frac{\kappa/k - 1/2}{\kappa/k + 1/2}.$$

To keep the article light and readable, we present our arguments in the context of Theorem 1.1 first and then indicate the adjustments needed for the proof of Theorem 1.3 in Section 3.3.

2. PRELIMINARIES

Notation. Throughout the paper, $\epsilon > 0$ denotes a parameter which may be chosen to be as small as we like, but need not have the same value from one occurrence to another. The letter p denotes an odd prime and $q = p^k$. We use μ_{p-1} to denote the set of $(p-1)^{\text{th}}$ roots of unity in the p -adic integers \mathbb{Z}_p . All implicit constants may depend on ϵ , p and the parameter θ introduced in (1.8), but not on k .

2.1. Approximate functional equations. We have the following standard approximate functional equations.

Lemma 2.1. *For a primitive Dirichlet character χ modulo q , let ι be defined by $\chi(-1) = (-1)^\iota$, and let*

$$(2.1) \quad \begin{aligned} U(x) &= \frac{1}{2\pi i} \int_{(2)} \frac{\Gamma(\frac{s+\iota}{2} + \frac{1}{4})}{\Gamma(\frac{\iota}{2} + \frac{1}{4})} (\pi^{\frac{1}{2}} x)^{-s} \frac{ds}{s}, \\ V(x) &= \frac{1}{2\pi i} \int_{(2)} \frac{\Gamma(\frac{s+\iota}{2} + \frac{1}{4})^2}{\Gamma(\frac{\iota}{2} + \frac{1}{4})^2} (\pi x)^{-s} \frac{ds}{s}. \end{aligned}$$

We have that

$$(2.2) \quad U(x) \ll_c x^{-c}, \quad V(x) \ll_c x^{-c}$$

for any $x, c > 0$. For any $\lambda > 0$, we have that

$$(2.3) \quad L(\tfrac{1}{2}, \chi) = \sum_{n \geq 1} \frac{\chi(n)}{n^{\frac{1}{2}}} U\left(\frac{n}{q^{1+\lambda}}\right) + O(q^{-100}),$$

$$(2.4) \quad |L(\tfrac{1}{2}, \chi)|^2 = 2 \sum_{n_1, n_2 \geq 1} \frac{\chi(n_1) \overline{\chi}(n_2)}{(n_1 n_2)^{\frac{1}{2}}} V\left(\frac{n_1 n_2}{q}\right),$$

where the implied constant in (2.3) depends on λ .

Proof. The first equation (2.3) is established by the functional equation of $L(s, \chi)$, which may be found in [9, Theorem 4.15], together with [9, Theorem 5.3], in which we take $G(u) = 1$ and $X = q^{\frac{1}{2} + \lambda}$. With this choice of X , the second sum in [9, (5.12)] may be bounded by q^{-100} . The second equation is established by applying [9, Theorem 5.3] to the product $L(s, \chi)L(s, \overline{\chi})$, rather than to each factor individually, with $G(u) = 1$ and $X = 1$. The estimates (2.2) may be found in [9, Proposition 5.4]. \square

The sums in (2.3) and (2.4) are essentially restricted to $n < q^{1+\lambda+\epsilon}$ and $n_1 n_2 < q^{1+\epsilon}$, by (2.2).

2.2. Character averages. In this section, we record the orthogonality relations provided by averaging over the family of Dirichlet characters in a Galois orbit; see Lemma 2.3 below. We start with a familiar auxiliary result.

Lemma 2.2. *Let m and $k \geq 1$ be integers. If $p^k \mid (m^p - 1)$, then $p^{k-1} \mid (m - 1)$.*

Proof. The claim is trivially true for $m = 1$, so assume $m > 1$. Since $m \equiv m^p \equiv 1 \pmod{p}$, we may write $m = 1 + p^r t$ for some $r \geq 1$ and some integer t with $p \nmid t$. Then we have

$$m^p - 1 = (1 + p^r t)^p - 1 \equiv p^{r+1} t \pmod{p^{r+2}},$$

so that p^{r+1} is the highest power of p that divides $m^p - 1$. In particular, since $p^k \mid (m^p - 1)$, we get $r + 1 \geq k$, and so $r \geq k - 1$ and $p^{k-1} \mid (m - 1)$. \square

Lemma 2.3. *Let $q = p^k$ for an odd prime p and let \mathcal{O} be any Galois orbit of primitive Dirichlet characters mod q . For any integer n , we have that*

$$(2.5) \quad \sum_{\chi \in \mathcal{O}} \chi(n) = 0$$

unless

$$(2.6) \quad n^{p-1} \equiv 1 \pmod{p^{k-1}}.$$

Proof. Suppose that \mathcal{O} has cardinality given by (1.3), for some $d \mid (p - 1)$. We first show that (2.5) holds unless

$$(2.7) \quad n^{p(p-1)} \equiv 1 \pmod{q}.$$

It was shown in [6, pg 17] that

$$(2.8) \quad \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} \chi(n) = \frac{\mu(\text{ord}(n^{\frac{p-1}{d}}))}{\phi(\text{ord}(n^{\frac{p-1}{d}}))},$$

where $\text{ord}(n^{\frac{p-1}{d}})$ denotes the multiplicative order of $n^{\frac{p-1}{d}}$ in the group $(\mathbb{Z}/q\mathbb{Z})^\times$. Since $|(\mathbb{Z}/q\mathbb{Z})^\times| = p^{k-1}(p - 1)$, if (2.7) is not satisfied, then p^2 divides $\text{ord}(n^{\frac{p-1}{d}})$, and so (2.8) is zero.

Now if (2.7) holds, then Lemma 2.2 implies, by taking $m = n^{p-1}$, that (2.6) holds. \square

Note that the condition (2.6), which is all we will need from our orthogonality relations, requires less information than what is provided by the full sum over all $\chi \in \mathcal{O}$ or the explicit evaluation (2.8). This will be transparent in Lemma 3.1, which features a thinner average and for which we provide an independent proof.

2.3. Mollifiers. The starting point of the mollifier method is the observation that

$$(2.9) \quad \frac{1}{|\mathcal{O}|} \sum_{\substack{\chi \in \mathcal{O} \\ L(\frac{1}{2}, \chi) \neq 0}} 1 \geq \frac{1}{|\mathcal{O}|} \sum_{\substack{\chi \in \mathcal{O} \\ L(\frac{1}{2}, \chi) M(\chi) \neq 0}} 1 \geq \frac{\left| \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} L(\frac{1}{2}, \chi) M(\chi) \right|^2}{\frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} |L(\frac{1}{2}, \chi)|^2 |M(\chi)|^2}.$$

The second inequality above is the Cauchy-Schwarz inequality. The next step of the method is to evaluate the mollified moments. We prove the following.

Proposition 2.4. *Let $q = p^k$ for an odd prime p and let \mathcal{O} be any Galois orbit of primitive Dirichlet characters mod q . For $0 \leq \theta < 1$ in (1.8), we have that*

$$\frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} L(\frac{1}{2}, \chi) M(\chi) = 1 + O(q^{-\frac{1}{4}+\epsilon} + q^{-\frac{1}{2}+\frac{\theta}{2}+\epsilon}).$$

Proposition 2.5. *Let $q = p^k$ for an odd prime p and let \mathcal{O} be any Galois orbit of primitive Dirichlet characters mod q . Suppose that $\chi(-1) = (-1)^\iota$ for any $\chi \in \mathcal{O}$. For $0 \leq \theta < \frac{1}{2}$ in (1.8), we have that*

$$\begin{aligned} \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} |L(\frac{1}{2}, \chi)|^2 |M(\chi)|^2 &= \frac{p-1}{p} \sum_{\substack{m_1, m_2 \leq q^\theta \\ (m_1 m_2, q)=1}} \frac{a_{m_1} \bar{a}_{m_2}}{[m_1, m_2]} \left(\log \left(\frac{q(m_1, m_2)^2}{\pi m_1 m_2} \right) + C \right) \\ &\quad + O(q^{-\frac{1}{4}+\epsilon} + q^{-\frac{1}{2}+\theta+\epsilon}), \end{aligned}$$

where (m_1, m_2) denotes the greatest common divisor of m_1 and m_2 , $[m_1, m_2] = \frac{m_1 m_2}{(m_1, m_2)}$ denotes the least common multiple of m_1 and m_2 , and $C = \frac{\Gamma'(\frac{1+2\iota}{4})}{\Gamma(\frac{1+2\iota}{4})} + 2\gamma + 2\frac{\log p}{p-1}$.

The final step is to insert the main terms of Propositions 2.4 and 2.5 into the ratio on the right hand side of (2.9), and then choose the coefficients a_m so that the ratio is maximized. We note that the main terms of our mollified moments are identical to those in Iwaniec and Sarnak's problem (see [10, (5.5)]) because in both problems the main terms arise from the diagonal contributions. That is, if $\chi(-1) = (-1)^\iota$ for all $\chi \in \mathcal{O}$, we have for any $0 \leq \theta < \frac{1}{2}$ and some $\delta > 0$ depending on p and θ that

$$\begin{aligned} \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} L(\frac{1}{2}, \chi) M(\chi) - \frac{2}{\varphi^*(q)} \sum_{\substack{\chi \bmod q \\ \chi(-1)=(-1)^\iota}}^* L(\frac{1}{2}, \chi) M(\chi) &\ll q^{-\delta}, \\ \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} |L(\frac{1}{2}, \chi)|^2 |M(\chi)|^2 - \frac{2}{\varphi^*(q)} \sum_{\substack{\chi \bmod q \\ \chi(-1)=(-1)^\iota}}^* |L(\frac{1}{2}, \chi)|^2 |M(\chi)|^2 &\ll q^{-\delta}, \end{aligned}$$

where \sum^* means that summation is restricted to the primitive characters and $\varphi^*(q) = \sum_{\chi \bmod q}^* 1$. The optimal choice for a_m will therefore be the same as in Iwaniec and Sarnak's problem (and we will not repeat the proof of this here), which yields that the ratio on the right hand side of (2.9) is $\frac{\theta}{1+\theta} + o(1)$ as $k \rightarrow \infty$. Taking $\theta \rightarrow \frac{1}{2}$, Theorem 1.1 thus follows from Propositions 2.4 and 2.5.

2.4. Roth's theorem. The following lemma is a special case of a result of Rohrlich [15, Proposition 1, pg 401]. It is a consequence of the p -adic version of Roth's theorem, due to Ridout [14].

Lemma 2.6. *Let $\beta \in \mathbb{Z}_p$ and $0 < \delta < \frac{1}{2}$. Suppose that β is algebraic over \mathbb{Q} of degree at least 2. Then, for sufficiently large $k \geq k_0(\beta, \delta)$, there are no nonzero integers a and b which satisfy*

$$|a - b\beta|_p \leq p^{-k+1}$$

and

$$|a|, |b| < (p^k)^{\frac{1}{2}-\delta}.$$

Proof. In [15, Proposition 1, pg 401], take $\alpha_p = 1$ and $\beta_p = \beta$. Note that condition (ii) directly above the proposition is satisfied because $\beta \notin \mathbb{Q}$. Note that k_0 is not computable. \square

When $(b, p) = 1$, this result says that an approximation of the algebraic number β by $\frac{a}{b}$ to an error within $(\max\{|a|, |b|\})^{-2-\delta}$ is too good to exist. Note that there are infinitely many approximations of any $\beta \in \mathbb{Z}_p$ up to within $\ll (\max\{|a|, |b|\})^{-2}$ by a p -adic incarnation of Dirichlet's Approximation Theorem (see also [2] for an analogue of the Farey dissection in this context), and it is a hallmark of Roth's theorem that the exponent in Lemma 2.6 is essentially the best possible. For an interesting investigation into existence of algebraic numbers exhibiting approximability by rationals within the transition range between the exponents -2 and $-2 - \delta$, see [11].

We stress that the p -adic analogues of previous partial results toward Roth's Theorem, such as the theorems of Liouville, Thue, Siegel, and Dyson, do not (except for a few small primes p) suffice to obtain an asymptotic in the situation of Proposition 2.5 or Theorem 1.2 with our methods. This is so because, for example when estimating (3.12), in order to obtain (3.13) with a $o(1)$ -upper bound on the right-hand side for large q , we need to be able to take Q (essentially the allowable length of intervals in Lemma 2.7, below) to be at least $(p^k)^{\frac{1}{4}+\delta}$, whereas all results prior to the actual p -adic Roth's theorem furnish only $(p^k)^{o_p(1)}$.

We will also use the following convenient implication of Lemma 2.6.

Lemma 2.7. *Let $0 < \delta < \frac{1}{2}$, let $k \geq k_1(\delta)$ be sufficiently large, and let \mathcal{A}_k and \mathcal{B}_k be intervals in the rational integers of length at most $(p^k)^{\frac{1}{2}-\delta}$. Then there are at most $p-3$ pairs $(a, b) \in \mathcal{A}_k \times \mathcal{B}_k$ such that*

$$(ab, p) = 1,$$

$$(2.10) \quad a \not\equiv \pm b \pmod{p^{k-1}},$$

and

$$(2.11) \quad a^{p-1} - b^{p-1} \equiv 0 \pmod{p^{k-1}}.$$

Proof. Suppose that a and b satisfy the conditions of the lemma. The congruence (2.11) implies that the p -adic integer $a^{p-1} - b^{p-1}$ has norm

$$(2.12) \quad |a^{p-1} - b^{p-1}|_p = \left| \prod_{\zeta \in \mu_{p-1}} (a - b\zeta) \right|_p \leq p^{-k+1}.$$

Recall that the roots of unity in μ_{p-1} are distinct modulo p . By this fact and the assumption $(ab, p) = 1$, we have that $a - b\zeta$ and $a - b\zeta'$ are distinct modulo p for $\zeta \neq \zeta'$. Thus, by (2.12) and (2.10), for some $\zeta \in \mu_{p-1} \setminus \{\pm 1\}$ we have

$$|a - b\zeta|_p \leq p^{-k+1}.$$

Now suppose for a contradiction that at least $p-2$ pairs (a, b) satisfy the conditions of the lemma. Then by the argument above and Dirichlet's Box Principle, we have for some $\zeta \in \mu_{p-1} \setminus \{\pm 1\}$, at least two distinct pairs $(a_1, b_1), (a_2, b_2) \in \mathcal{A}_k \times \mathcal{B}_k$ satisfying

$$|a_j - b_j \zeta|_p \leq p^{-k+1} \quad (j = 1, 2).$$

It follows from the strong triangle inequality that

$$|(a_2 - a_1) - (b_2 - b_1)\zeta|_p \leq \max\{|a_1 - b_1 \zeta|_p, |a_2 - b_2 \zeta|_p\} \leq p^{-k+1}.$$

We also have, by the assumption on the lengths of \mathcal{A}_k and \mathcal{B}_k , that

$$|a_2 - a_1|, |b_2 - b_1| \leq (p^k)^{\frac{1}{2}-\delta}.$$

Thus by Lemma 2.6, in which we take $\beta = \zeta$, we deduce that for $k > k_1$ sufficiently large, where k_1 is not computable, we must have $a_2 - a_1 = b_2 - b_1 = 0$. This is the desired contradiction. \square

3. PROOFS OF THE MAIN RESULTS

3.1. Proof of Proposition 2.4. In Lemma 2.1, let $\lambda > 0$ be such that $\lambda + \theta < 1$. We have that

$$(3.1) \quad \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} L(\tfrac{1}{2}, \chi) M(\chi) = \sum_{m \leq q^\theta} \sum_{n \geq 1} \frac{a_m}{(nm)^{\frac{1}{2}}} U\left(\frac{n}{q^{1+\lambda}}\right) \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} \chi(nm) + O(q^{-99}).$$

Note that the exchange of summation above is valid because although the function $U(x)$ depends on $\chi(-1)$, this value is the same for every character in \mathcal{O} . Now, by Lemma 2.3, we have that

$$\frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} \chi(nm) = 0$$

unless $(nm)^{p-1} \equiv 1 \pmod{p^{k-1}}$, in which case we have by Hensel's Lemma that nm is congruent to one of $\zeta_1, \dots, \zeta_{p-1} \in \mu_{p-1}$ modulo $p^{k-1}\mathbb{Z}$. Separating the term $nm = 1$ for the main term in Proposition 2.4, and using also the divisor bound, we have that (3.1) equals

$$(3.2) \quad U\left(\frac{1}{q^{1+\lambda}}\right) + O\left(q^\epsilon \sum_{1 \leq j \leq p-1} \sum_{\substack{1 < s \leq q \\ s \equiv \zeta_j \pmod{p^{k-1}}}} s^{-\frac{1}{2}}\right) + O\left(q^\epsilon \sum_{1 \leq j \leq p-1} \sum_{\substack{q < s < q^{1+\lambda+\theta+\epsilon} \\ s \equiv \zeta_j \pmod{p^{k-1}}}} s^{-\frac{1}{2}}\right).$$

By shifting the line of integration in (2.1) to $\Re(s) = -\frac{1}{2} + \epsilon$, we see that the main term above equals $1 + O(q^{-\frac{1}{2}+\epsilon})$.

The summands in the first error term are particularly sensitive to the size of s . From the condition that $s^{p-1} \equiv 1 \pmod{p^{k-1}}$ and $s > 1$, we immediately have that $s > p^{\frac{k-1}{p-1}}$, and the first error term is seen to be

$$O\left(q^{-\frac{1}{2(p-1)}+\epsilon}\right),$$

without recourse to p -adic Roth's theorem. However, we can improve this estimate by appealing to Lemma 2.6. The terms with $s \equiv \pm 1 \pmod{p^{k-1}}$, $s > 1$, contribute $O(p^{-(k-1)/2})$. As for the terms corresponding to $s \equiv \zeta_j \not\equiv \pm 1 \pmod{p^{k-1}}$, Lemma 2.6 with $\beta = \zeta_j$ guarantees that, for sufficiently large k , there are no values of $|s| < (p^k)^{\frac{1}{2}-\delta}$ with $|s - \zeta_j \cdot 1|_p \leq p^{-k+1}$, so that all these terms must in fact satisfy $s \geq (p^k)^{\frac{1}{2}-\delta}$, and in total the first error term is

$$O\left(q^{-\frac{1}{4}+\frac{1}{2}\delta+\epsilon}\right).$$

Finally, writing $s = \zeta_j + p^{k-1}r$, we have that the second error term above is bounded by

$$q^\epsilon \sum_{1 \leq r < q^{\lambda+\theta+\epsilon}} (qr)^{-\frac{1}{2}} \ll q^{\frac{\lambda+\theta-1}{2}+\epsilon}.$$

Taking the positive λ and δ to be as small as we like and adjusting the implied constants completes the proof. \square

3.2. Proof of Proposition 2.5. By Lemma 2.1, we have that

$$(3.3) \quad \begin{aligned} & \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} |L(\tfrac{1}{2}, \chi)|^2 |M(\chi)|^2 \\ &= 2 \sum_{m_1, m_2 \leq q^\theta} \sum_{n_1, n_2 \geq 1} \frac{a_{m_1} \bar{a}_{m_2}}{(n_1 n_2 m_1 m_2)^{\frac{1}{2}}} V\left(\frac{n_1 n_2}{q}\right) \frac{1}{|\mathcal{O}|} \sum_{\chi \in \mathcal{O}} \chi(n_1 m_1) \bar{\chi}(n_2 m_2). \end{aligned}$$

We write this as a sum of diagonal terms and off-diagonal terms,

$$\sum_{n_1 m_1 = n_2 m_2} + \sum_{n_1 m_1 \neq n_2 m_2}.$$

The diagonal. We first consider the diagonal terms. The equality $n_1 m_1 = n_2 m_2$ is the same as requiring $n_1 = r m_2 / (m_1, m_2)$ and $n_2 = r m_1 / (m_1, m_2)$ for some $r \in \mathbb{N}$. Thus the diagonal contribution is

$$\sum_{n_1 m_1 = n_2 m_2} = 2 \sum_{\substack{m_1, m_2 \leq q^\theta \\ (m_1 m_2, p)=1}} \frac{a_{m_1} \bar{a}_{m_2}}{[m_1, m_2]} \sum_{\substack{r \geq 1 \\ (r, p)=1}} \frac{1}{r} V\left(\frac{r^2 m_1 m_2}{q(m_1, m_2)^2}\right).$$

The innermost sum above can be evaluated by the calculation in [10, Lemma 4.1] and equals

$$\frac{p-1}{2p} \left(\log \left(\frac{q(m_1, m_2)^2}{\pi m_1 m_2} \right) + C \right) + O\left(\left(\frac{q(m_1, m_2)^2}{m_1 m_2} \right)^{-\frac{1}{2}+\epsilon} \right),$$

where C is as in the statement of Proposition 2.5. The main term above gives the main term of Proposition 2.5, and the total error is less than

$$q^\epsilon \sum_{m_1, m_2 \leq q^\theta} \frac{1}{[m_1, m_2]} \left(\frac{q(m_1, m_2)^2}{m_1 m_2} \right)^{-\frac{1}{2}} \ll q^{-\frac{1}{2}+\epsilon} \sum_{m_1, m_2 \leq q^\theta} \frac{1}{(m_1 m_2)^{\frac{1}{2}}} \ll q^{-\frac{1}{2}+\theta+\epsilon}.$$

The off-diagonal. We now turn to the off-diagonal contribution, which we must bound by a negative power of q . By Lemma 2.3 and (2.2), we have that

$$\sum_{n_1 m_1 \neq n_2 m_2} \ll q^\epsilon \sum_{\substack{m_1, m_2 \leq q^\theta, n_1 n_2 \leq q^{1+\epsilon} \\ (n_1 n_2 m_1 m_2, p)=1 \\ (n_1 m_1)^{p-1} \equiv (n_2 m_2)^{p-1} \pmod{p^{k-1}} \\ n_1 m_1 \neq n_2 m_2}} \frac{1}{(n_1 n_2 m_1 m_2)^{\frac{1}{2}}}.$$

Writing $a = n_1 m_1$ and $b = n_2 m_2$ and splitting the resulting sum above into dyadic intervals $A \leq a < 2A$ and $B \leq b < 2B$, it suffices to show that the sum

$$(3.4) \quad \frac{q^\epsilon}{(AB)^{\frac{1}{2}}} \sum_{\substack{A \leq a < 2A \\ B \leq b < 2B \\ (ab, p)=1 \\ a^{p-1} \equiv b^{p-1} \pmod{p^{k-1}} \\ a \neq b}} 1$$

is less than a negative power of q for

$$(3.5) \quad 1 \leq AB \leq q^{1+2\theta+\epsilon}.$$

We split (3.4) further as

$$(3.6) \quad \frac{q^\epsilon}{(AB)^{\frac{1}{2}}} \sum_{\substack{A \leq a < 2A \\ B \leq b < 2B \\ (ab, p)=1 \\ a \equiv \pm b \pmod{p^{k-1}} \\ a \neq b}} 1 \quad + \quad \frac{q^\epsilon}{(AB)^{\frac{1}{2}}} \sum_{\substack{A \leq a < 2A \\ B \leq b < 2B \\ (ab, p)=1 \\ a^{p-1} \equiv b^{p-1} \pmod{p^{k-1}} \\ a \not\equiv \pm b \pmod{p^{k-1}}}} 1.$$

In the first sum above, we must have $2A > p^{k-1}$ or $2B > p^{k-1}$. In the first case, for each of the B choices for b , there are $O(\frac{A}{q})$ choices for a by the Chinese Remainder Theorem. In the same way in the second case there are $O(\frac{AB}{q})$ choices for a and b . Thus the first sum in (3.6) is bounded by

$$\frac{q^\epsilon}{(AB)^{\frac{1}{2}}} \frac{AB}{q} \ll q^{-\frac{1}{2}+\theta+\epsilon}.$$

Now we consider the second sum in (3.6). We must show that

$$(3.7) \quad \frac{q^\epsilon}{(AB)^{\frac{1}{2}}} \sum_{\substack{A \leq a < 2A \\ B \leq b < 2B \\ (ab, p)=1 \\ a^{p-1} \equiv b^{p-1} \pmod{p^{k-1}} \\ a \not\equiv \pm b \pmod{p^{k-1}}}} 1$$

is bounded by a negative power of q . We may assume that

$$(3.8) \quad q^{-\frac{1}{2}} < \frac{A}{B} < q^{\frac{1}{2}},$$

since otherwise the proof is complete. To see this, suppose without loss of generality that $A \leq B$. Then for each of the A choices of a in (3.7), there are $O(1 + \frac{B}{q})$ possibilities of b which satisfy the congruence $a^{p-1} \equiv b^{p-1} \pmod{p^{k-1}}$. Thus if (3.8) is not satisfied, then (3.7) is bounded by

$$(3.9) \quad \frac{q^\epsilon}{(AB)^{\frac{1}{2}}} \left(A + \frac{AB}{q} \right) \ll q^{-\frac{1}{4}+\epsilon} + q^{-\frac{1}{2}+\theta+\epsilon}.$$

Now, assuming (3.8), we analyze (3.7) according to the sizes of A and B as follows. Let $0 < \delta < \frac{1}{p}$ and $Q = q^{\frac{1}{2}-2\delta}$.

Case 1. Suppose that $2A < q^{\frac{1}{2}-\delta}$ and $2B < q^{\frac{1}{2}-\delta}$. Every term in (3.7) would have to satisfy $a \equiv b\zeta_j \pmod{p^{k-1}}$ for some $\zeta_j \in \mu_{p-1} \setminus \{\pm 1\}$, and hence $|a - b\zeta_j|_p \leq p^{-k+1}$ with $|a|, |b| < (p^k)^{\frac{1}{2}-\delta}$. For sufficiently large k , however, by Lemma 2.6 there are no such nonzero integers a and b , and the corresponding sum (3.7) is actually empty.

Case 2. Suppose that $2A \geq q^{\frac{1}{2}-\delta}$ and $2B < q^{\frac{1}{2}-\delta}$. (The case $2A < q^{\frac{1}{2}-\delta}$ and $2B \geq q^{\frac{1}{2}-\delta}$ is treated similarly). Dividing the dyadic interval $A \leq a < 2A$ into smaller pieces of length Q , we may bound (3.7) by

$$(3.10) \quad \frac{q^\epsilon}{(AB)^{\frac{1}{2}}} \sum_{1 \leq u \leq \frac{A}{Q}} \sum_{\substack{A+(u-1)Q \leq a < A+uQ \\ B \leq b < 2B \\ (ab,p)=1 \\ a^{p-1} \equiv b^{p-1} \pmod{p^{k-1}} \\ a \not\equiv \pm b \pmod{p^{k-1}}}} 1.$$

By Lemma 2.7, the innermost sum of (3.10) is, for sufficiently large k , bounded by a constant (depending on p). Using this fact and (3.8), we see that (3.10) is bounded by

$$(3.11) \quad \frac{q^\epsilon}{(AB)^{\frac{1}{2}}} \frac{A}{Q} \ll q^{-\frac{1}{4}+2\delta+\epsilon}.$$

This falls into the error term of Proposition 2.5 as we may take δ to be as small as we like.

Case 3. Suppose that $2A \geq q^{\frac{1}{2}-\delta}$ and $2B \geq q^{\frac{1}{2}-\delta}$. Dividing the dyadic intervals $A \leq a < 2A$ and $B \leq b < 2B$ into smaller pieces of length Q , we may rewrite (3.7) as

$$(3.12) \quad \frac{q^\epsilon}{(AB)^{\frac{1}{2}}} \sum_{\substack{1 \leq u \leq \frac{A}{Q} \\ 1 \leq v \leq \frac{B}{Q}}} \sum_{\substack{A+(u-1)Q \leq a < A+uQ \\ B+(v-1)Q \leq b < B+vQ \\ (ab,p)=1 \\ a^{p-1} \equiv b^{p-1} \pmod{p^{k-1}} \\ a \not\equiv \pm b \pmod{p^{k-1}}}} 1.$$

By Lemma 2.7, the innermost sum of (3.12) is, for sufficiently large k , bounded by a constant (depending on p). Using this fact and (3.5), we see that (3.12) is bounded by

$$(3.13) \quad \frac{q^\epsilon}{(AB)^{\frac{1}{2}}} \frac{AB}{Q^2} \ll q^{-\frac{1}{2}+\theta+4\delta+\epsilon}.$$

This falls into the error term of Proposition 2.5 as we may take δ to be as small as we like.

The proof of Proposition 2.5 is now complete. \square

3.3. The case of thin orbits. In this section, we prove Theorem 1.3. As is customary in analytic number theory (and as is already the case with full Galois orbits of primitive characters), the principal change introduced by the shrinking family of characters in the orbit \mathcal{O}_κ is that more terms survive averaging over the family. We quantify this effect with the following modification of Lemma 2.3 on orthogonality relations.

Lemma 3.1. *Let $q = p^k$ for an odd prime p , let $0 < \kappa \leq k-1$, and let \mathcal{O}_κ be a thin Galois orbit of primitive Dirichlet characters mod q . For any integer n , we have that*

$$(3.14) \quad \sum_{\chi \in \mathcal{O}_\kappa} \chi(n) = 0$$

unless

$$(3.15) \quad n^{p-1} \equiv 1 \pmod{p^{\tilde{\kappa}+1}},$$

where $\tilde{\kappa} = \min(\kappa, k-2)$.

Proof. Fix a character $\chi_0 \in \mathcal{O}_\kappa$. Fix a generator g of the cyclic group $(\mathbb{Z}/p^k\mathbb{Z})^\times$, and write $\chi_0(g) = \xi^\gamma$ for some γ . In particular, $(\gamma, \phi(q)) = (p-1)/d$, where $d \mid (p-1)$ is the order of χ_0 and of all characters in \mathcal{O}_κ , so that the corresponding full orbit $\mathcal{O} \supseteq \mathcal{O}_\kappa$ has cardinality given by (1.3).

If n is an integer divisible by p , the lemma is trivially true. We therefore assume n is relatively prime to p and let $0 \leq r < p^{k-1}(p-1)$ be such that $n = g^r$ in $(\mathbb{Z}/p^k\mathbb{Z})^\times$. From (1.12), it is immediate that

$$\sum_{\chi \in \mathcal{O}_\kappa} \chi(n) = \sum_{\substack{a \bmod p^{k-1}(p-1) \\ a \equiv 1 \bmod p^{k-1-\kappa}(p-1)}} \xi^{\gamma r a} = \begin{cases} \chi_0(n) \sum_{0 \leq j < p^\kappa} e(\gamma r j / p^\kappa), & 0 \leq \kappa < k-1, \\ \chi_0(n)^p \sum_{0 \leq j < p^{k-1}, p \nmid j} e(\gamma r j / p^{k-1}), & \kappa = k-1. \end{cases}$$

In either case, the resulting sum vanishes unless $p^{\tilde{\kappa}} \mid r$. The condition $p^{\tilde{\kappa}} \mid r$ is equivalent to $n^{p^{k-1-\tilde{\kappa}}(p-1)} \equiv 1 \bmod p^k$, which by Lemma 2.2 implies that $n^{p-1} \equiv 1 \bmod p^{\tilde{\kappa}+1}$. This proves the lemma. \square

We will only use (3.15) as a condition modulo p^κ . In particular, note that the localization (2.6) is achieved already by averaging over $\chi \in \mathcal{O}_{k-1}$. The resulting Ramanujan sum in the case $\kappa = k-1$ should be compared with the explicit evaluation (2.8).

The analogs of Propositions 2.4 and 2.5 on mollified moments are as follows:

Proposition 3.2. *Let $q = p^k$ for an odd prime p , let $k/2 < \kappa \leq k-1$, and let \mathcal{O}_κ be a thin Galois orbit of primitive Dirichlet characters mod q . For $0 \leq \theta < 2(\frac{\kappa}{k} - \frac{1}{2})$ in (1.8), we have*

$$\frac{1}{|\mathcal{O}_\kappa|} \sum_{\chi \in \mathcal{O}_\kappa} L(\tfrac{1}{2}, \chi) M(\chi) = 1 + O(q^{-\frac{\kappa}{4k} + \epsilon} + q^{\frac{1}{2} + \frac{\theta}{2} - \frac{\kappa}{k} + \epsilon}),$$

while, for $0 \leq \theta < \frac{\kappa}{k} - \frac{1}{2}$ in (1.8), we have

$$\begin{aligned} \frac{1}{|\mathcal{O}_\kappa|} \sum_{\chi \in \mathcal{O}_\kappa} |L(\tfrac{1}{2}, \chi)|^2 |M(\chi)|^2 &= \frac{p-1}{p} \sum_{\substack{m_1, m_2 \leq q^\theta \\ (m_1 m_2, q)=1}} \frac{a_{m_1} \bar{a}_{m_2}}{[m_1, m_2]} \left(\log \left(\frac{q(m_1, m_2)^2}{\pi m_1 m_2} \right) + C \right) \\ &\quad + O(q^{-\frac{\kappa}{4k} + \epsilon} + q^{\frac{1}{2} + \theta - \frac{\kappa}{k} + \epsilon}), \end{aligned}$$

with notations as in Proposition 2.5.

Proof. The proof follows the proofs of Propositions 2.4 and 2.5, with Lemma 3.1 as the orthogonality relation in place of Lemma 2.3.

For the first mollified moment, we start by inserting the approximate functional equation as in (3.1). By Lemma 3.1, the character average isolates the main term, which comes from $mn = 1$ and is identical as before, and summands with $s = mn \equiv \zeta_j \bmod p^\kappa$, $s > 1$, which we split into two terms, corresponding to the ranges $1 < s \leq p^\kappa$ and $p^\kappa < s < q^{1+\lambda+\theta+\epsilon}$. By Lemma 2.6, for sufficiently large k , all summands in the first sum satisfy $s \geq (p^\kappa)^{\frac{1}{2}-\delta}$, and in total the first error term is $O((p^\kappa)^{-\frac{1}{4}+\frac{1}{2}\delta})$. Writing $s = \zeta_j + p^\kappa r$, the second error term is similarly bounded by

$$q^\epsilon \sum_{1 \leq r < q^{1+\lambda+\theta+\epsilon-\kappa/k}} (p^\kappa r)^{-\frac{1}{2}} \ll q^{\frac{\lambda+\theta+1}{2} - \frac{\kappa}{k}},$$

completing the proof of the first part of our proposition.

As for the second mollified moment, we start by expanding using the same functional equation (3.3). The main term arises from the diagonal terms, when $n_1 m_1 = n_2 m_2$, and is the same

as above, while in the off-diagonal terms we are left by Lemma 3.1 with the sums as in (3.4) now subject to $a^{p-1} \equiv b^{p-1} \pmod{p^\kappa}$, and which we further split as in (3.6). In the first sum, over $a \equiv \pm b \pmod{p^\kappa}$, we must have $2A > p^\kappa$ or $2B > p^\kappa$, and the total contribution from these terms is bounded by

$$\frac{q^\epsilon}{(AB)^{\frac{1}{2}}} \frac{AB}{p^\kappa} \ll q^{\frac{1}{2} + \theta - \frac{\kappa}{k} + \epsilon}.$$

In the second sum, analogously as before, we may assume that $p^{-\frac{\kappa}{2}} < A/B < p^{\frac{\kappa}{2}}$, since otherwise the proof is complete as in (3.9). We now set $Q = (p^\kappa)^{\frac{1}{2} - 2\delta}$ and consider three cases. If $2A < (p^\kappa)^{\frac{1}{2} - \delta}$ and $2B < (p^\kappa)^{\frac{1}{2} - \delta}$, then the sum is empty for sufficiently large k by Lemma 2.6. If $2A \geq (p^\kappa)^{\frac{1}{2} - \delta}$ and $2B < (p^\kappa)^{\frac{1}{2} - \delta}$, then by splitting the a -sum into intervals of length Q the sum is bounded as in (3.11) by

$$\frac{q^\epsilon}{(AB)^{\frac{1}{2}}} \frac{A}{Q} \ll q^{-\frac{\kappa}{4k} + 2\delta + \epsilon},$$

and, finally, if both $2A \geq (p^\kappa)^{\frac{1}{2} - \delta}$ and $2B \geq (p^\kappa)^{\frac{1}{2} - \delta}$, then the sum is bounded as in (3.13) by

$$\frac{q^\epsilon}{(AB)^{\frac{1}{2}}} \frac{AB}{Q^2} \ll q^{\frac{1}{2} + \theta - \frac{\kappa}{k} + 4\delta \frac{\kappa}{k} + \epsilon},$$

which completes the proof as we may take δ as small as we wish. \square

Theorem 1.3 now follows from Proposition 3.2 in the same way in which Theorem 1.1 is deduced from Propositions 2.4 and 2.5, by taking $\theta \rightarrow \frac{\kappa}{k} - \frac{1}{2}$.

Acknowledgements. Part of this work was done during the excellent National Science Foundation-supported 29th Automorphic Forms Workshop held at the University of Michigan, Ann Arbor; we wish to express our thanks to the organizers of the conference. The third author is grateful to Jeffrey C. Lagarias for his constant encouragement.

REFERENCES

1. R. Balasubramanian and V. Kumar Murty, *Zeros of Dirichlet L -functions*, Ann. Sci. École Norm. Sup. (4) **25** (1992), no. 5, 567–615.
2. V. Blomer and D. Milićević, *p -adic analytic twists and strong subconvexity*, Ann. Sci. École Norm. Sup. (4), to appear.
3. H. Bohr and E. Landau, *Sur les zéros de la fonction $\zeta(s)$ de Riemann.*, C. R. Acad. Sci., Paris **158** (1914), 106–110.
4. C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over \mathbf{Q} : wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).
5. H. M. Bui, *Non-vanishing of Dirichlet L -functions at the central point*, Int. J. Number Theory **8** (2012), no. 8, 1855–1881.
6. G. Chinta, *Analytic ranks of elliptic curves over cyclotomic fields*, J. Reine Angew. Math. **544** (2002), 13–24.
7. H. Davenport, *Multiplicative number theory*, third ed., Graduate Texts in Mathematics, vol. 74, Springer-Verlag, New York, 2000, Revised and with a preface by Hugh L. Montgomery.
8. R. Greenberg, *On the critical values of Hecke L -functions for imaginary quadratic fields*, Invent. Math. **79** (1985), no. 1, 79–94.
9. H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.
10. H. Iwaniec and P. Sarnak, *Dirichlet L -functions at the central point*, Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, pp. 941–952.
11. J. C. Lagarias, *A complement to Ridout's p -adic generalization of the Thue-Siegel-Roth theorem*, Analytic number theory (Philadelphia, Pa., 1980), Lecture Notes in Math., vol. 899, pp. 264–275.

12. D. Milićević, *Sub-Weyl subconvexity for Dirichlet L -functions to prime power moduli*, Compositio Math., to appear.
13. A. G. Postnikov, *On the sum of characters with respect to a modulus equal to a power of a prime number*, Izv. Akad. Nauk SSSR. Ser. Mat. **19** (1955), 11–16.
14. D. Ridout, *The p -adic generalization of the Thue-Siegel-Roth theorem*, Mathematika **5** (1958), 40–48.
15. D. E. Rohrlich, *On L -functions of elliptic curves and anticyclotomic towers*, Invent. Math. **75** (1984), no. 3, 383–408.
16. ———, *On L -functions of elliptic curves and cyclotomic towers*, Invent. Math. **75** (1984), no. 3, 409–423.
17. A. Selberg, *On the zeros of Riemann's zeta-function*, Skr. Norske Vid. Akad. Oslo I. (1942), no. 10, 59 pp.
18. G. Shimura, *The special values of the zeta functions associated with cusp forms*, Comm. Pure Appl. Math. **29** (1976), no. 6, 783–804.
19. ———, *On the periods of modular forms*, Math. Ann. **229** (1977), no. 3, 211–221.
20. ———, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kanô Memorial Lectures, 1.
21. K. Soundararajan, *Nonvanishing of quadratic Dirichlet L -functions at $s = \frac{1}{2}$* , Ann. of Math. (2) **152** (2000), no. 2, 447–488.
22. R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.
23. A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

SCIENCE PROGRAM, TEXAS A&M UNIVERSITY AT QATAR, PO Box 23874, DOHA, QATAR
E-mail address: rizwanur.khan@qatar.tamu.edu, hieu.ngo@qatar.tamu.edu

DEPARTMENT OF MATHEMATICS, BRYN MAWR COLLEGE, 101 NORTH MERION AVENUE, BRYN MAWR, PA 19010, U.S.A
E-mail address: dmilicevic@brynmawr.edu